



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
|-----------------|-------------|----------------------|---------------------|------------------|

10/759,182

01/20/2004

John Brawner Duffie III

10-008

7709

23164

7590

06/26/2006

LEON R TURKEVICH

2000 M STREET NW

7TH FLOOR

WASHINGTON, DC 200363307

EXAMINER

SERRAO, RANODHI N

ART UNIT

PAPER NUMBER

2141

DATE MAILED: 06/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | | |
|------------------------------|------------------------|---------------------|--|
| Office Action Summary | Application No. | Applicant(s) | |
| | 10/759,182 | DUFFIE ET AL. | |
| | Examiner | Art Unit | |
| | Ranodhi Serrao | 2141 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 April 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-35 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-35 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

1. Applicant's arguments, see remarks, filed 24 April 2006, with respect to the rejection(s) of claim(s) 1-35 under Title 35 U.S.C. have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of newly found prior art reference(s). See rejections below.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over MeLampy et al. (2003/0051130) and Bacha et al. (6,795,920).

4. As per claim 1, MeLampy et al. teaches a method in a router having at least one outbound interface (see MeLampy et al., ¶ 5), the method comprising: establishing, on the outbound interface, a plurality of Internet Protocol (IP)-based secure connections with respective destinations based on receiving encrypted packets generated by a cryptographic module (see MeLampy et al., ¶ 27), each encrypted packet successively output from the cryptographic module having a corresponding successively-unique sequence number (see MeLampy et al., ¶ 55); (2) reordering, in each queuing module,

a corresponding group of the data packets associated with the corresponding secure connection (see MeLampy et al., ¶ 40) according to a determined quality of service policy (see MeLampy et al., ¶ 36) and based on a corresponding assigned maximum output bandwidth for the corresponding queuing module (see MeLampy et al., ¶ 34), and (3) outputting to the cryptographic module the group of data packets, from each corresponding queuing module according to the corresponding assigned maximum output bandwidth, for generation of the encrypted packets (see MeLampy et al., ¶ 33-34); and second outputting the encrypted packets from the cryptographic module to the one outbound interface for transport via their associated secure connections (see MeLampy et al., ¶ 57). But fails to teach controlling supply of data packets to the cryptographic module by: (1) assigning, for each secure connection, a corresponding queuing module. However, Bacha et al. teaches controlling supply of data packets to the cryptographic module by: (1) assigning, for each secure connection, a corresponding queuing module (see Bacha et al., col. 9, lines 45-48). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify MeLampy et al. to controlling supply of data packets to the cryptographic module by: (1) assigning, for each secure connection, a corresponding queuing module in order to allow user processes running in dedicated vaults to communicate with other User processes running in different vaults using a secure depositor running as a module in a vault process in each vault (see Bacha et al., abstract).

5. As per claim 10, MeLampy et al. teaches a router comprising: a cryptographic module configured for successively outputting encrypted packets having respective

Art Unit: 2141

successively-unique sequence numbers (see MeLampy et al., ¶ 40); an outbound interface configured for establishing a plurality of Internet Protocol (IP)-based secure connections with respective destinations based on receiving respective streams of the encrypted packets (see MeLampy et al., ¶ 27); each queuing module configured for: (1) outputting to the cryptographic module a corresponding group of the data packets associated with the corresponding secure connection, and according to a corresponding assigned maximum output bandwidth for the corresponding queuing module, for generation of the corresponding stream of the encrypted packets (see MeLampy et al., ¶ 33-36), and (2) reordering the corresponding group of the data packets according to a determined quality of service policy and the corresponding assigned maximum output bandwidth (see MeLampy et al., ¶ 61). But fails to teach a queue controller configured for controlling supply of data packets to the cryptographic module, the queue controller configured for assigning, for each secure connection, a corresponding queuing module: However, Bacha et al. teaches a queue controller configured for controlling supply of data packets to the cryptographic module, the queue controller configured for assigning, for each secure connection, a corresponding queuing module (see Bacha et al., col. 9, lines 45-48). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify MeLampy et al. to a queue controller configured for controlling supply of data packets to the cryptographic module, the queue controller configured for assigning, for each secure connection, a corresponding queuing module in order to allow user processes running in dedicated vaults to communicate with other

User processes running in different vaults using a secure depositor running as a module in a vault process in each vault (see Bacha et al., abstract).

6. Claims 2-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over McLampy et al. and Bacha et al. as applied to claim 1 above, and further in view of Young et al. (2003/0093563).

7. As per claim 2, McLampy et al. and Bacha et al. teach the mentioned limitations of claim 1 above but fail to teach a method, wherein the reordering step includes, in each queuing module, reordering the corresponding group of the data packets according to the determined quality of service policy in response to detection of a congestion condition in the outbound interface. However, Young et al. teaches a method, wherein the reordering step includes, in each queuing module, reordering the corresponding group of the data packets according to the determined quality of service policy in response to detection of a congestion condition in the outbound interface (see Young et al., ¶ 9). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify McLampy et al. and Bacha et al. to a method, wherein the reordering step includes, in each queuing module, reordering the corresponding group of the data packets according to the determined quality of service policy in response to detection of a congestion condition in the outbound interface in order to implement a complete customer premise solution that enables secure, reliable and manageable delivery of voice, video and data services over common IP connections (see Young et al., ¶ 2).

8. As per claims 3-9, the above-mentioned motivation of claim 2 applies fully in order to combine MeLampy et al., Bacha et al. and Young et al.

9. As per claim 3, MeLampy et al. and Bacha et al.-Young et al. teach a method, wherein the reordering step includes, in each queuing module: establishing a plurality of queues having respective identified priorities (see Young et al., paragraph 0051); storing each data packet associated with the corresponding secure connection in one of the queues based on a corresponding identified priority for said each data packet (see Young et al., paragraph 0019); and selectively outputting the stored data packets from the queues, according to the corresponding quality of service policy (see Young et al., paragraph 0009).

10. As per claim 4, MeLampy et al. and Bacha et al.-Young et al. teach a method, wherein: the establishing step includes establishing, on each of a plurality of the outbound interfaces (see Young et al., paragraph 0080), a corresponding plurality of the secure connections with a corresponding plurality of respective destinations based on receiving a corresponding stream of encrypted packets from the cryptographic module (see Young et al., paragraph 0082); the controlling step includes controlling the supply of data packets, for each outbound interface, from the cryptographic module based on repeating the assigning, reordering, and outputting steps for each of the secure connections (see Young et al., paragraph 0150); the second outputting step including outputting each encrypted packet to a corresponding one of the outbound interfaces according to a routing decision executed by the router (see Young et al., paragraph 0098).

11. As per claim 5, McLampy et al. and Bacha et al.-Young et al. teach a method, wherein the second outputting step includes outputting the encrypted packets for transport via their associated secure connections according to IP Security (IPSEC) protocol (see Young et al., paragraph 0123).

12. As per claim 6, McLampy et al. and Bacha et al.-Young et al. teach a method, wherein the determined quality of service policy implements a guaranteed quality of service for one of a video stream and an audio stream (see Young et al., paragraph 0053).

13. As per claim 7, McLampy et al. and Bacha et al.-Young et al. teach a method, wherein the audio stream is a Voice over IP media stream (see Young et al., paragraph 0053).

14. As per claim 8, McLampy et al. and Bacha et al.-Young et al. teach a method, wherein the controlling step further includes obtaining, for each queuing module, the corresponding assigned maximum output bandwidth from a configuration register (see Young et al., paragraph 0051).

15. As per claim 9, McLampy et al. and Bacha et al.-Young et al. teach a method, wherein the controlling step further includes negotiating, for at least one queuing module, the corresponding assigned maximum output bandwidth with the corresponding destination (see Young et al., paragraphs 0085-0087).

16. Claims 11-35 have similar limitations as to claims 1-10, therefore, they are being rejected under the same rationale.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ranodhi Serrao whose telephone number is (571)272-7967. The examiner can normally be reached on 8:00-4:30pm, M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571)272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


RUPAL DHARIA
SUPERVISORY PATENT EXAMINER